

Automated Commercial Environment—Requirements Recommendation

Date:	July 27, 2001
Number:	ITD-017
Requestor:	ITDS Sub-Committee
Customs Co-Chair:	Don Kusser
Trade Co-Chair:	Tom Anastasi and Sandra Scott

Requirement

Account Access

The ITDS system must allow access to information and functions through an Account structure. To clarify this requirement, individual Agencies and the Trade are Accounts within the system. Authorized users within the Agencies and the Trade organizations are Clients. Clients are given explicit roles that allow them to access certain portions of the information, work rules and processes owned by any of the Accounts and/or shared by any number of Accounts.

Through the account structure, Agencies and the Trade are able to manage all aspects of their relationships between each client and the tasks necessary to collaborate/communicate around information with every other Account. Owners can open Accounts and identify users of the system (clients) after registration with the ITDS consortia and/or after registration with an individual Agency. Only registered Accounts and their users can gain access to information and functions in the ITDS system.

Accounts shall be able to define their organizational structure subsidiaries and work groups and assign roles to clients within the structure. These roles are group-level permissions enabling clients assigned by the Account owners to access certain information and functions that are available within the Account. The Account owner, upon registration of a client or upon a number of other events, can explicitly determine and declare what access to any information and functions that any client has. Role-based security is preferable to user-based, as administration costs and time are reduced due to simplified control of permissions.

The information provided to open an Account and to establish access shall be verified through the use of U.S. Government-agency accepted procedures (electronic and/or manual) to ensure that only authorized and authenticated parties who have registered to open and own accounts and identify users/clients gain access to ITDS. Once an Account is authorized and verified and clients identified, a system-wide process grants or denies each request for access.

Accounts shall be able to authorize any other Account (s) to collaborate or work on the information in their span of control as well as to work on the common information that exists within the ITDS system.

Agency/ITDS system administrators (who will act under the rules of their agency and/or the ITDS agency consortia) shall have certain expanded capabilities to supervise Accounts and Clients. These administrators will be specially configured and Clients and will be assigned their roles by the Agencies and/or the Agency ITDS Consortia.

All account activity shall be captured in a series of access audit logs and transactional audit records. This requires a structure that supports versioning of Account information and transactional views of it. Each Account will have a record of the versions of their transactional views and shall be able to recreate their transactions using time-based selection criterion.

Business Need

To create an account structure that defines the business, payment, regulatory status information and relationships between each trade member and each of the agencies. To enforce the authentication of ITDS account owners and their clients. To provide the means for the agencies and the trade to each control access to their information within the system. All are integral to providing a computer system that will be useable, accurate, and auditable and at the same time a system secure from unauthorized access and prevent the misuse of data or functions.

The provision of Account-based permission to access information and functions allows the Account owners, agencies and trade partners to collaborate around a shared set of consistent information. This controlled access to common information will alleviate the need for error-prone data re-entry.

Technical Need

The Account relationships and abstractions need to be designed into the core data and applications architecture. The account structure must be part of the core architecture at the data and object model level. If this is not done the application will not be efficient, secure, extensible or adaptable. The proper expression and definition of the Account structure at the appropriate level in the application architecture will simplify data management, allow for secure collaboration and speed application development of the core application and any extensions.

Benefits

Provides a sound and time-proof infrastructure that allows each Account to control and experience a private and personalized view of the Account status and information at the user interface level through a browser and/or when further fully integrated with existing legacy systems.

Provides a safe, secure and trusted information sharing and transaction-processing structure that creates utility for the agencies and for the trade.

Facilitates the rapid creation of Accounts and allows for account-based transaction processing, supervision and Account management.

Provides both the trade and the agencies a means to audit and evaluate account-based performance.

Allows for the reuse and sharing of the core common client and entity information that describes these Accounts among the agencies and the controlled sharing of a consistent view of the core common data elements used by each of the Accounts owned by the agencies and the trade participants.

Risks

If role-based Security and Account Access processes are not built into ITDS, the system will become prone to fraud, will be inaccurate and un-auditable.

Related Subcommittees

This section lists the names of any subcommittee that may have an interest in the requirement recorded.

Priority: **Critical** ☒ **High** ☐ **Medium** ☐ **Low** ☐

Customs Use Only

Approved ☐

Not Approved ☐

Further Evaluation Required ☐